แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต ๒
รอบการประเมินที่ ๒/๒๕๖๗ ตั้งแต่วันที่ ๑ เมษายน – ๓๐ กันยายน ๒๕๖๗
ประจำปีงบประมาณ พ.ศ.๒๕๖๗

ชื่อ-นามสกุล นางสาวพัชนิดา มณฑาทอง **ตำแหน่ง** นักวิชาการเกษตรปฏิบัติการ
หน่วยงาน สถานีพัฒนาที่ดินฉะเชิงเทรา
หัวข้อการพัฒนา การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness)
วิธีการพัฒนา ผ่านสื่อการเรียนการสอน online
วันที่พัฒนา ๑๔ สิงหาคม ๒๕๖๗ **สถานที่** online
หน่วยงานที่จัดอบรม สถาบันพัฒนาบุคลากรด้านดิจิทัลภาครัฐ หรือ TDGA
วัตถุประสงค์

๑. เพื่อให้ผู้เรียนมีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
๒. เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับภัยคุกคามประเภทต่าง ๆ และแนวทางป้องกันแก้ไข
๓. เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

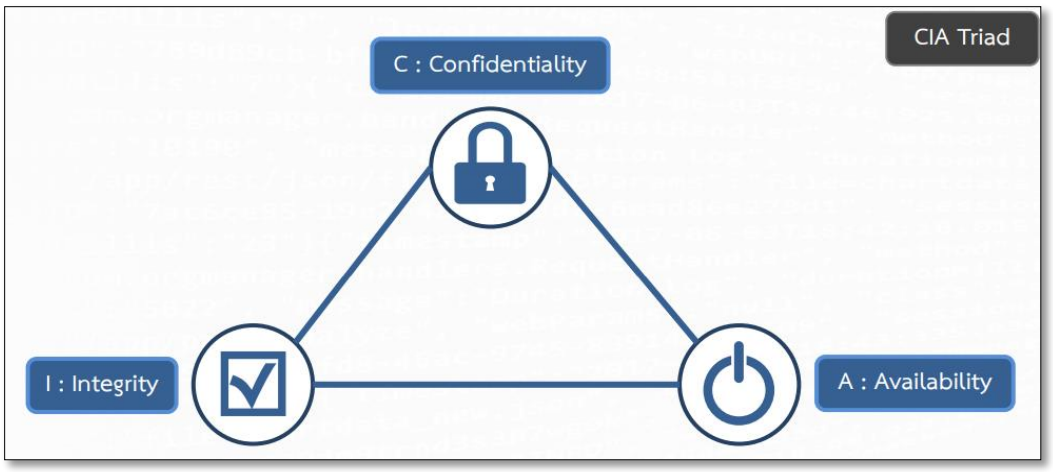
สรุปสาระสำคัญ

Cybersecurity หรือ ความมั่นคงปลอดภัยทางไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี มาตรการที่ใช้ปกป้องระบบคอมพิวเตอร์ อุปกรณ์อิเล็กทรอนิกส์ ข้อมูล และระบบเครือข่ายจากการถูกเข้าถึงโดยบุคคลที่ไม่มีสิทธิ์ การโจมตี และความเสี่ยงทางไซเบอร์ที่อาจส่งผลกระทบต่อความปลอดภัยในสารสนเทศและเทคโนโลยีขององค์กร หรือบุคคลทั่วไป รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้นและความเสียหายให้กับองค์กร

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์
- พ.ร.บ.การรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ๒๕๖๒
- พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐
- พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
- มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

๑.ความรู้พื้นฐานของ CyberSecurity

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ CIA Triad หรือ CIA Model ซึ่งประกอบด้วยตัว ซี(C) ตัวไอ(I) และตัวเอ(A)



C : Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุด ข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้

I : Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มี ความถูกต้องอย่างต่อเนื่อง

A : Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการ ให้บริการข้อมูล

๒. รูปแบบภัยคุกคามของ CyberSecurity

Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่ เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูล ไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่างๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการ ผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง

- ไวรัส (Virus)
- เวิร์ม (Worms)
- โทรจัน (Trojans)

Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไข เว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็น เว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware เว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น Code ของเว็บไซต์เช่น CMS หรือ Web Server หรือ Database Server

Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญ หรือก่อกวน

DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกันจุดประสงค์ที่ทำเพื่อให้เว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชันหรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ

Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่าง ๆ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต

Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่าน ที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน

๑. สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล

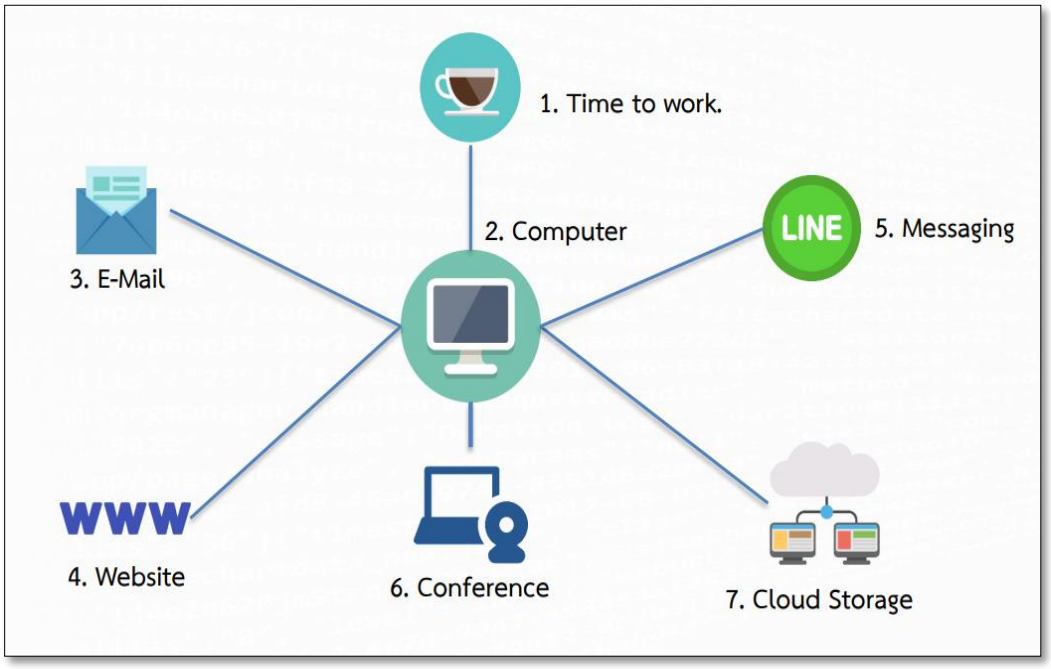
๒. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ

๓. ก่อนเปิดไฟล์ต่าง ๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทำการเปิด

Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่าง ๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวณผลเพื่อสร้างรายได้กลับไปที่ Hacker

๓. ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

- วันทำงาน
- วันพักผ่อน



๑. วันทำงาน

Computer

๑. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล

๒. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

๓. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ

๔. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๖. ไม่ควรจด Password หรือติด Password ไว้ที่หน้าจอ และไม่ควรบอก Password แก่ผู้อื่น

E-mail

๑. ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

๒. ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจนไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค

๓. ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค

๔. Gmail - Report Spam Mail

๕. Gmail - Report Phishing Mail

Website สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่าง ๆ

๒. ไม่ควรทำการบันทึก Password ต่าง ๆ บน Browser

๓. เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น

๔. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น

๕. ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ

๖. ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing

๗. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

Messaging สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรบันทึก Password ไว้ที่โปรแกรม

๒. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง

๓. มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่าง ๆ ที่ได้รับมา

๔. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

Fake News Fake News ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือ ซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE, Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น

วิธีการสังเกตข่าวปลอม

๑. มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ

๒. ระบุที่มาของข่าวไม่ได้

๓. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์

๔. สำนวนการเขียนออกแนวการโฆษณา

Conference สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ใช้สถานที่เหมาะสมกับการ Conference

๒. ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง

๓. แชร์เอกสารต่างๆ อย่างระมัดระวัง

๔. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน

๕. มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

Cloud Storage สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. แยก User ในการใช้งานของแต่ละบุคคล

๒. ควรก าหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น

๓. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น

๔. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

๖. มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

๒. วันพักผ่อน

Computer สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล

๒. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

๓. ควรติดตั้ง anti-malware และมีการอัพเดตอย่างสม่ำเสมอ

๔. มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

๕. มีการอัพเดทเวอร์ชั่นของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๖. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ

๗. มีการใช้ Password ที่ดีและไม่ควรบอก Password แก่ผู้อื่น

Free WIFI สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรใช้งาน WiFi ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน

๒. หลีกเลี่ยงการใช้งาน WiFi ที่ไม่รู้ที่มาในการให้บริการ

Mobile สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. เปิดการใช้งาน PIN/Password,Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์

๒. ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา

๓. กำหนด Application permission ให้เหมาะสม

๔. มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างเหมาะสม

๕. มีการอัพเดทเวอร์ชั่นของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

Internet Connection สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน

๒. เปลี่ยน SSID และรหัสผ่านของ WiFi ที่กำหนดมาจากผู้ให้บริการ

๓. กำหนดผู้ที่สามารถเข้าใช้งานอินเทอร์เน็ตเท่าที่จำเป็น

IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการทำงานร่วมกับระบบต่าง ๆ หรือแอปพลิเคชันต่าง ๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้อง มีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. เปลี่ยน Default Password ที่มาจากโรงงาน

๒. ควรมีการอัพเดทเฟิร์มแวร์ให้เป็นเวอร์ชั่นล่าสุด

๓. ใช้ application ที่ใช้ในการคอนโทรลกับอุปกรณ์ต่าง ๆ ให้เป็นเวอร์ชั่นล่าสุด

ประโยชน์ที่ได้รับจากการพัฒนาความรู้

การสร้างความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ที่เกิดขึ้น จะเห็นว่าสิ่งที่เราต้องทำคือเราต้องมีความรู้เกี่ยวกับภัยคุกคามประเภทต่าง ๆ และแนวทางป้องกันแก้ไข เพื่อให้สามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและนำไปปฏิบัติตามเพื่อความปลอดภัยในชีวิตประจำวัน

(นางสาวพัชนิดา มณฑาทอง)
นักวิชาการเกษตรปฏิบัติการ

(นายบุญสม พรหมสุวรรณ์)
ผู้อำนวยการสถานีพัฒนาที่ดินฉะเชิงเทรา